*Kriminalističke teme*
*Zbornik radova*
Godina XIX, Broj 5, 2019.
ISSN 1512-5505



# ULOGA PSIHOLOGIJE U UNAPREĐENJU CYBER SIGURNOSTI
THE ROLE OF PSYCHOLOGY IN ENHANCING CYBERSECURITY

**Pregledni naučni rad**

**Doc. dr. Elvira Čekić[180]**

**SAŽETAK**

Inspiracija za rad i problem (i) koji se radom oslovljava (ju):
Online okruženje je značajan činilac svakodnevnog ponašanja i aktivnosti pojedinaca i organizacija u savremenom ljudskom društvu. Pojava naglašenog posredovanja u komunikaciji povećava rizike i razvija negativna iskustva sa kojima se susreću korisnici, posebno mladi. U tom smislu online okruženje značajno doprinosi pojavi kriminalnog i nasilnog ponašanja (npr. uznemiravanje, seksualno iskorištavanje, prevare, hakovanje). Stoga je veoma bitna uloga psihologije u unapređenju cyber sigurnosti.
Ciljevi rada (naučni i /ili društveni):
Naučni cilj ovog istraživanja je da ostvari saznanje o uzročno-posljedičnom odnosu pojava online komunikacije i devijantnih, uključujući i kriminalne oblike ponašanja.
Društveni cilj je da istraživanja svojim rezultatima doprinesu razumijevanju ljudskog ponašanja u virtualnom prostoru, pri čemu psihologija istražuje i proučava promjene u ponašanju na individualnom i kolektivnom nivou.
Metodologija/Dizajn:
U istraživanju metodološki pristup je zasnovan na shvatanjima savremene socijalne psihologije.
Ograničenja istraživanja/rada:
Imajući u vidu da informatički stručnjaci i psiholozi sve više zajedno djeluju u oblasti interakcije pojedinca sa računarom, cyber psihologija značajnije je polje istraživanja. Ipak, zagovornici i stručnjaci u oblasti cyber psihologije i dalje se suočavaju sa problemima multidisciplinarnosti i transdisciplinarnosti (npr. Kibernetika-računari). Naučnici iz različitih disciplina gledaju na iste pojave sa različitih perspektiva, te se ponekad njihovo shvatanje i jezik razlikuje toliko da je teško postići optimalnu i prihvatljivu saglasnost.
Rezultati/Nalazi:
Na osnovu dosadašnjih rezultata istraživanja i proučavanja naučno-saznajnog fonda, evidentan je zabrinjavajući porast cyber kriminala u svijetu, što potvrđuje i činjenica da je nešto manje od oko 2/3 populacije postalo žrtva nekog od oblika cyber kriminala.
Generalni zaključak:

180 doktor psiholoških nauka, docent na Fakultetu za kriminalistiku, kriminologiju i sigurnosne studije, Univerziteta u Sarajevu. Izvodi nastavu iz više naučnih disciplina iz oblasti psiholoških nauka - Psihologija, Forenzička psihologija, Psihologija kriminaliteta, Psihologija ličnosti i Socijalna psihologija. e-mail: ecekic@fkn.unsa.ba

Razumijevanjem uticaja savremenih tehnologija na ljudsko ponašanje u virtualnom prostoru psihologija je utvrdila značajne promjene u ponašanju na individualnom i kolektivnom nivou.
Opravdanost istraživanja/rada:
Uloga Cyber psihologije je značajno polje istraživanja, koje se bavi psihološkim uticajima i implikacijama kompjuterskih i online tehnologija na pojavu raznih i raznovrsnih oblika devijantnog ponašanja.

**Ključne riječi**
cyber psihologija, cyber sigurnost, online ponašanje, cyber kriminal, viktimizacija, ljudski faktor

**ABSTRACT**
Inspiration behind the paper and the issue (s) it addresses:
The online environment is a significant factor which takes part in the daily behavior and activities of individuals and organizations in the modern human society. The emergence of online communication increases risks and develops experiences of negative encounters among users, especially young people. In this regard, the online environment significantly contributes to a serious emergence of criminal and violent behavior (eg harrasment, sexual exploitation, fraud, hacking). Therefore, the role of psychology in enhancing cybersecurity is very important.
Rresearch objectives (scientific and/or social):
The scientific aim of this research is to examine the causal link between online communication and deviant, including criminal forms of behavior.
The social aim of the results of this reseach is to contribute to the understanding of human behavior in a virtual space, whereby psychology explores and studies the changes in behavior at the individual and collective levels.
Methodology/Design:
The methodological approach in this research is based on perceptions of contemporary social psychology.
Limitations of the research/paper:
Given the fact that information technology experts and psychologists increased their mutual cooperation in the field of interaction of individuals with computers, however, cyberpsychology is a more significant field of research. Nevertheless, advocates and experts in cyberpsychology continue to face issues regarding multidisciplinarity and transdisciplinarity (eg. cybernetics-computers). Scientists from different disciplines look at the same phenomena from different perspectives, and sometimes their understanding and language differs in a way that it is difficult to achieve an optimal and acceptable consent.
Results/Findings:
On the basis of results from previous research and of studying scientific and cognitive information, there is an alarming rise in cybercrime in the world, as confirmed by the fact that something under 2/3 of the population has become the victim of some type of cybercrime.
General conclusion:
Through understanding the influence of modern technologies on human behavior in the virtual space, psychology identified significant changes in behavior at individual and collective levels.
Justification of the research/paper:

The role of cyberpsychology is a significant field of research addressing the psychological impacts and implications of computer and online technologies on the emergence of various and diverse forms of deviant behavior.

**Key words**
cyberpsychology, cybersecurity, online behavior, cyber crime, victimization, human factor

## UVOD

Naslov – odredbe naslova teme nas obavezuju na istraživanje (u ovom slučaju dominantno teorijsko sa činiocima empirijskog uvida i saznanja) psihologije, odnosno posebno socijalne psihologije u procesu unapređenja i razvoja sistema personalne, ali i institucionalne zaštite od cyber kriminala.

U samom pristupu proučavanja identifikovanog problema suočavamo se s određenim problemima, kao što su pripadnost teme nauci – naučnoj disciplini, problem sigurnosti i bezbjednosti, problemima ljudskog i društvenog ponašanja, koji uključuju činioce individualne i društvene svijesti i društvene i pojedinačne volje kao bitnih komponenti ljudskog i društvenog ponašanja, itd.

Da bi govorili o sigurnosti i bezbjednosti svakako treba poći od činjenice ugrožavanja ljudi i ljudskih zajednica, njihove imovine i svojine, te u tom smislu problem sigurnosti, odnosno sigurnost je prema svim važećim savremenim relevantnim društvenim teoretičarima i teorijama jedna od osnovnih, primarnih ljudskih, društvenih potreba. Čovjek i ljudsko društvo se ostvaruju u mnoštvu sfera u ljudskom i društvenom i u svakoj od tih sfera života čovjek i društvo teže za sigurnošću. To ispoljavanje težnje za sigurnošću i društvenom bezbjednošću se mora posmatrati u dva osnovna vida: pasivna i aktivna sigurnost. Ukoliko se radi o sigurnosnoj situaciji u kojoj subjekti – ljudi i njihova imovina i svojina nisu ugroženi od prirodnih sila ili društvenih subjekata, onda bi takvu situaciju smatrali pasivnom bezbjednošću, jer je ona zaštićena angažovanjem nekih trećih subjekata. U savremenom društvu, u većini slučajeva, obični građani su uživaoci pasivne bezbjednosti – sigurnosti. Dok se proces aktivne bezbjednosti – sigurnosti ostvaruje preko države i njenih sistema ili/i međunarodnih sistema bezbjednosti.

Priroda i čovjek su istovremeno izvor i predmet ugrožavanja i sigurnosti i ugroženosti. Stoga savremeno društvo poznaje situacije sa zaštićenim i nezaštićenim dijelom prirode i zaštićenim i posebno zaštićenim dijelom ljudi – ljudskog društva. Mi se u radu ne bavimo ugrožavanjem prirode i prirodom kao nosiocem ugrožavanja, već čovjekom koji svojim ponašanjem i djelanjem ugrožava druge ljude – pojedince, društvene grupe, ljudske zajednice, organizacije i institucije društva. Razumijevajući ljudsko ponašanje u virtuelnom prostoru, u kome je ljudski faktor „najslabija karika sigurnosti u cyber (virtuelnom) prostoru“, pri čemu je 70% ukupne populacije u svijetu imalo pristup internetu do 2017“, psihologija na više načina („podizanje javne svijesti o rizicima cyber sigurnosti u cilju

prilagođavanja percepcije ljudi i, posljedično, njihovog ponašanja prema privatnosti"; „razumijevanje uticaja cyber kriminala na ponašanje žrtava u procesu viktimizacije" i dr.) može utvrditi promjene u ponašanju na individualnom i kolektivnom nivou, pri čemu, istražujući ljudsku prirodu, ona ima ključnu ulogu u ublažavanju tog rizika (Wederhold, 2014).

Psihologija je složena nauka o ponašanju ljudi i drugih živih bića, koja otkriva i razumije unutrašnje razloge i spoljne poticaje, iz fizičkog socijalnog i online okruženja, na određena ponašanja. Nije naš zadatak da se u kontekstu obrade predmetnog konglomerata problema bavimo problemom definicije predmeta psihologije i njene klasifikacije, ali to ćemo učiniti u mjeri u kojoj se ukazuje na ulogu i značaj psihologije (korpusa psiholoških nauka) koja obuhvata ukupnu psihologiju ljudi. Pritom, treba imati u vidu da su oblasti društvenih i psiholoških nauka neodvojivi, međusobno povezani i prožeti i da su u bliskom odnosu sa prirodnim naukama, naročito sa prirodnim naukama koje se bave živom prirodom.

Ljudsko saznanje je tvorevina ljudskog uma i ljudskog djelanja, to znači ljudske psihe i ljudskog organizma u kome postoje organi neophodni za odgovarajuće opažanje i percepciju, promišljanje i zaključivanje. Ustvari, to je ljudski mozak i živčani sistem.

U okviru psihologije postoji veliki broj psihologijskih grana i disciplina. Jedna od njih je i Socijalna psihologija, za koju Zvonarević (1976) tvrdi da je to "grana psihologije koja proučava psihološke aspekte pojava i socijalne aspekte psiholoških pojava".

U Psihologijskom rječniku na str. 449-450, se kaže da je socijalna psihologija "grana ili disciplina psihologije … Kao opći predmet socijalne psihologije određuje se socijalna psihologija čovjeka, njegov socijalni razvoj, socijalno ponašanje, društveni život ljudi ili uzajamno djelovanje …"

U samom središtu socijalne psihologije je **pojava socijalnog uticaja**, te se socijalna psihologija definira kao znanstvena disciplina **koja proučava kako stvarna ili zamišljena prisutnost drugih ljudi utiče na naše misli, osjećaje i ponašanje** (bold. E. Č.) (Allport, 1985; Aronson et al., 2005).

Odredbe citirane definicije najbliže i najpreciznije ukazuju na predmet socijalne psihologije, koja je od posebnog značaja u ostvarivanjima ljudskog i društvenog ponašanja, djelanja i njihovim društvenim interakcijama. Dakle, u sticanju i praktikovanju – primjeni (sa)znanja pored ljudskih čula kao organa i nagona neophodan je um. A izučavanje uma se svodi na proučavanje mozga (kao organa) i nervnog sistema i ponašanja u raznim sistemima i raznim situacijama. Sposobnosti (obdarenost, afinitet, itd.) uma su različiti a izvori razlika nepoznati, osim za jedan faktor koji nazivamo obrazovanje i vaspitanje ili kako ga upravo naziva socijalna psihologija "socijalizacija" (Termiz, 2013).

Prema tome, značaj i uloga psihologije, odnosno socijalne psihologije se ogleda u formiranju i razvoju ličnosti individue (izgradnja socijalizovane ličnosti) i formiranju društveno prihvatljivih modela ponašanja u procesima ljudskih i društvenih interakcija i raznih oblika i načina društvenih komunikacija, uključujući i online komunikacije, kao bitan činilac njihove personalne, ali i grupne, institucionalne i organizacijske sigurnosti kao brane jednom od razvijenih savremenih oblika kriminala, kao što je cyber kriminal.

## 1. Definicija pojma sigurnost

Ne postoji univerzalno prihvaćena definicija cyber sigurnosti. Riječ, pojam, termin cyber sigurnost je složenica i ona se sastoji od pojma – termina "cyber" i "sigurnost", pri čemu je "cyber" prefiks i označava virtuelni prostor i odnosi se na elektronske komunikacione mreže i virtuelnu stvarnost (Oxford, 2014; Craigen et al., 2014). On je kao takav nastao od pojma "kibernetika", koji se odnosi na "polje kontrole i teorije komunikacije, bilo to među mašinama ili životinjama" (Wiener, 1948; Craigen et al., 2014). Kao virtuelni prostor bio je namijenjen i osmišljen kao okruženje za informacije" (Singer & Friedman, 2013), a „danas je proširena procjena cyber prostora". Tako, npr. Public Safety Canada (2010) definiše cyber prostor kao "elektronski svijet koji su stvarali međusobno povezane mreže informacijske tehnologije i informacije na tim mrežama". On „predstavlja globalno dobro u kome ljudi zajedno razmjenjuju ideje, usluge i prijateljstvo" (ukoliko nije to dobro zloupotrebljeno). "Cyber prostor nije statičan, već je dinamičan, evoluirajući, višerazinski ekosistem fizičke infrastrukture, softvera, propisa, ideja, inovacija i interakcija pod uticajem sve veće populacije saradnika, koji predstavlja spektar ljudskih namjera (Deibert & Rohozinski, 2010).

Pojam sigurnost teško je definirati u opštem smislu. Rasprave o sigurnosti, prema nekim autorima „nužno uključuju i nastoje razumjeti ko sekuritizira, o kojim pitanjima (prijetnjama), za koga (referentni objekt), zašto, s kojim rezultatima i pod kojim uslovima (Buzan, Waever i De Wilde, 1998). Može se govoriti o različitim oblicima sigurnosti (ljudskih osobina, fizičke sigurnosti, emocionalne sigurnosti, psihološke sigurnosti, sigurnosti informacijskih sistema, itd). Značenje termina sigurnosti je zasnovano na opažanju, mišljenju, znanju, osjećaju, vjerovanju, uvjerenju, sistemu vrijednosti, emocijama i personalnoj perspektivi.

Imajući u vidu polaznu, prethodno navedenu definiciju pojma sigurnosti, koja je vezana za situaciju pojedinca i njegovu koncepciju sigurnosti (aktuelno i perspektivno odsustvo lične ugroženosti, kao osnov za izvedeni pojam cyber sigurnosti), zapažamo da se ni teoretičari cyber sigurnosti nisu usaglasili, a time ni ponudili jednu, u osnovi, opšteprihvatljivu definiciju.

Prema dostupnoj savremenoj literaturi prisutne su sljedeće definicije cyber sigurnosti:

(1) "Cyber sigurnost uglavnom obuhvata odbrambene metode koje se koriste za otkrivanje i sprječavanje potencijalnih uljeza" (Kemmerer, 2003; Craigen et al., 2014);

(2) "Cyber sigurnost podrazumijeva zaštitu informatičkih mreža i informacija koje iste sadrže od prodora i od zlonamjernog oštećenja" (Lewis, 2006; Craigen et al., 2014);

(3) "Cyber sigurnost uključuje smanjenje rizika od zlonamjernog napada na softwer, kompjutere i mreže. To uključuje alate koji se koriste za otkrivanje pravila, zaustavljanje virusa, blokiranje zlonamjernog pristupa, provođenje provjere autentičnosti, omogućavanje šifrovanih komunikacija, itd." (Amoroso, 2006; Craigen et al., 2014);

(4) "Cyber sigurnost je skup instrumenata, politika, sigurnosnih koncepata, sigurnosnih mjera, smjernica, pristupa upravljanja rizicima, radnji, obuke, najboljih praksi, osiguranja tehnologija koje se mogu koristiti za zaštitu od cyber okruženja i organizacije i korisnikovih resursa" (ITU, 2009; Craigen et al., 2014);

(5) "Sposobnost zaštite ili odbrane upotrebe cyber-prostora od cyber-napada" (CNSS, 2010; Craigen et al., 2014);

(6) "Tehnologija, procesi, prakse i mjere za odgovor i ublažavanje koje su dizajnirane da zaštite mreže, računare, programe i podatke od napada, oštećenja ili neovlaštenog pristupa, kako bi se osigurala povjerljivost, integritet i dostupnost" (Public Safety Canada, 2014; Craigen et al., 2014);

(7) "Umijeće osiguranja postojanja i kontinuiteta informacijskog društva određene nacije, garantirajući i štiteći, u virtuelnom prostoru, informacije, imovinu i kritičnu infrastrukturu" (Canongia & Mandarino, 2014; Craigen et al., 2014);

(8) "Stanje zaštite od kriminalne ili neovlaštene upotrebe elektronskih podataka, ili mjere poduzete da se to postigne" (Oxford University Press, 2014; Craigen et al., 2014);

(9) "Aktivnost ili proces, sposobnost ili stanje prema kojem su informacioni i komunikacioni sistem i informacije sadržane u njemu zaštićene od i/ili zaštićene od oštećenja, neovlaštene upotrebe ili modifikacije ili eksploatacije" (DHS, 2014; Craigen et al., 2014);

Iz citiranih definicija cyber sigurnosti uočavamo njihove bitne odredbe: zaštite od kriminalne ili neovlaštene upotrebe podataka u procesu info-tehnologija u cyber prostoru, čime se faktički aktuelno i/ili potencijalno subjekti – ljudi kao pojedinci, grupe, ljudske zajednice i institucije ugroženi i čime se ugrožava njihov ljudski integritet, imovina i svojina.

To zahtijeva da se kompjuterska sigurnost fokusira na osiguranje tehnologije – sistema i komunikacijske infrastrukture, koja sadrži podatke i programe. Bitna komponenta informaciono – komunikacijskih tehnologija i sistema su ljudi, sigurnosno-bezbjednosna kultura i bezbjednosna politika i ponašanje subjekata, čije su bitne komponente svijest i volja u čemu, pored ostalog, psihologija, odnosno socijalna psihologija ima naglašeno značajnu ulogu.

## 2. Cyber kriminal

Odredbe naslova teme zahtijevaju da određenu pažnju posvetimo cyber kriminalu. Cyber kriminal se razlikuje od tradicionalnog ili klasičnog kriminala koji može biti počinjen na jednom određenom geografskom području. Cyber kriminal „se može počiniti na internetu i često nije jasno povezan sa geografskom lokacijom" (Wall, 2017; Jahankhani et al., 2014). Identifikaciju lokacije sa karakterističnim elementima kriminala gotovo je nemoguće utvrditi u cyber kriminalu.

U slučaju cyber kriminala prostorna karakteristika napadača se ne može ili je teže istu utvrditi, jer tzv. kompjuterski ili internet kriminal je "anti-prostorni". Stoga i jeste zadatak kriminologije razumijevanje motivacije kriminalaca analizom socijalnih karakteristika kriminalaca i njihovih prostornih lokacija. Pored kriminologije, u procesu razlikovanja sitnog lopova od profesionalnog kriminalnog hakera značajnu ulogu ima jasno utvrđena metodologija, koja treba obezbijediti pouzdanu vezu sa kompjuterskom forenzikom i psihologijom, koja će omogućiti otkrivanje i identifikaciju profila cyber kriminala i omogućiti razumijevanje njihovog ponašanja (Hemraj et al., 2012).

Prethodno navedenim se dovoljno jasno ukazuje na potrebu razlikovanja novih oblika od klasičnog kriminala, krivičnih djela koja su usmjerena na IT i počinjene putem IT (informacionih tehnologija) kao što su npr. hakiranje, prevare putem interneta (Holt, T., & Bossler, A., 2014; McGuire, M., & Dowling, 2013; Leukfeldt, 2017). Krivična djela počinjena putem interneta, kao što su: hakovanje, kreiranje borneta, zarazivanje kompjutera malwareom (zlonamjernim programima) su povezani sa tradicionalnim oblicima kriminala, – krivična djela prevare, prijetnje i uhođenja, a ponekad spadaju u obje kategorije kriminala – klasični i cyber kriminal.

Nesumnjivo je naglašen značaj cyber sigurnosti u savremenom društvu u kojem tzv. tehničkim napadima i nedopuštenim pristupima nosioci cyber kriminala dolaze do informacija od kojih imaju veliku korist. Informacije o kadrovskim registrima, kreditnim informacijama, poslovnim i drugim tajnama, šiframa, virtuelnom novcu, stanju na računu, itd. se prodaju, pa čak i više od jednom. Kriminalno pribavljene informacije se mogu koristiti za ucjenu i prodaju ukradenih informacija žrtvi (kao što je to naprimjer slučaj u kriminalu sa automobilima u klasičnom kriminalu) (Tikkanen, 2017).

Osnovne metode u cyber kriminalu su ubjeđivanje i manipulacija koja se koristi i u sprezi s ubjeđivanjem. Vještinom ubjeđivanja se obezbjeđuje dobra volja pojedinca i njegova spremnost da se pomogne. Dakle, ubjeđivanje je usmjereno na emociju žrtve. Manipulacija ima za cilj da preoblikuje percepcije druge osobe o nečemu, a njena svrha je da se ta osoba drži pod kontrolom (Hadnagy, Ch., & Ekman, P., 2014).

## 3. Cyber psihologija i ljudski faktori

Pojam cyber psihologija su utvrdili istraživači sredinom 1990-ih godina koji su proučavali online ponašanje. Imajući u vidu činjenicu da stručnjaci iz oblasti informatike i psiholozi „sve više djeluju u oblasti interakcije pojedinca sa računarom“, cyber psihologija je postala značajnije polje istraživanja (Widman, 2018).

Cyber psihologija je subdisciplina psihologije, koja proučava psihološke uticaje i implikacije kompjuterskih i online tehnologija, koje se odvijaju unutar virtuelnog, odnosno cyber prostora putem korištenja tehnologije (Attrill, 2016; Kaye, 2016; Widman, 2018).

Jedan od aspekata istraživanja i naučnog proučavanja je uticaj online okruženja na ponašanje i aktivnosti pojedinaca, ljudskih zajednica, institucija i organizacija. Ta posredovanost u komunikaciji (korištenje interneta) doprinosi povećanju rizika u manifestacijama raznih oblika devijantnih i kriminalnih ponašanja kao što su: uznemiravanje, seksualno iskorištavanje, prevare, hakovanje, zarazu malware-om, itd. (Bryce, 2015).

Da bi razumjeli online viktimizaciju i njeno prisustvo u kriminalnom ponašanju neophodno je poznavati bitne karakteristike online komunikacije a koje su vezane za pristup i pristupačnost savremenim IT, uslugama i aplikacijama koje predstavljaju sastavni dio digitalnog okruženja. Poznavanje bitnih karakteristika online interakcije je značajno zbog njihovog uticaja na ponašanje subjekata – ljudi, a koji aktuelno i potencijalno mogu doprinijeti kriminalnom ponašanju i viktimizaciji. U osnovne karakteristike online komunikacije mogu se svrstati: anonimnost, dezinhibicija, otkrivanje ličnih informacija, hiper intimnost, obmana, deindividualizacija, itd. (Bryce, 2015).

Nesumnjivo je da postoji visok nivo korelacije između online informacije i offline okruženja, u manifestaciji raznih oblika devijantnog i kriminalnog ponašanja i online ponašanja koja izlažu pojedinca riziku od viktimizacije. U online komunikacijama pojedinci dijele informacije koje se tiču njihovog identiteta, emocija, potreba, želja, namjera, aktivnosti, očekivanja, itd. Ta podjela značajnih personalnih informacija sa drugim, najčešće nepoznatim, u ovoj vrsti, visokorizičnih komunikacija se može koristiti u svrhe uznemiravanja, proganjanja, prevare, kompromitacije do hakiranja računara u bankama. Dakle, takva ponašanja u online komunikacijama doprinose narušavanju i/ili ugrožavanju tzv. cyber sigurnosti.

Rezultati savremenih istraživanja su, pored ostalog, utvrditi psihološku ranjivost pojedinaca kao posljedicu niskog stepena samopouzdanja, socijalne anksioznosti, depresije, te njihove socijalne situacije koju odlikuje haotična porodična situacija izazvana roditeljskim sukobima, razvodom braka i slično.

Polazeći od prethodno navedenog nameće se logično pitanje – a ko su to žrtve cyber kriminala, koji je to broj – kvalitet žrtava i obim krivičnih djela cyber kriminala? Istraživači cyber kriminala su otkrili postojanje značajne povezanosti između osobina ličnosti podložne napadima ove vrste kriminala, kao i vezu između podložnosti napadima socijalnog inžinjeringa i ključnih faktora ličnosti. Socijalni inžinjering se smatra upotrebom

manipulacije, uvjeravanja i utjecaja napadača kako bi se dobile osjetljive informacije ili kako bi se dobio pristup ograničenim područjima (Uebelacker and Quiel, 2014; Hadlington, 2017). Oni su predstavili teorijski okvir kojim ukazuju na direktnu povezanost između određenih osobina ličnosti (John and Srivastava, 1999; Hadlington, 2017) i osjetljivosti na socijalni inžinjering. Autori ukazuju na to da pojedinci koji posjeduju osobine kao što su: impulsivnost, ekstraverzija, otvorenost prema iskustvu i prihvatljivost su podložni napadima socijalnog inžinjeringa, dok su savjesnost, suglasnost, kritički odnos prema iskustvu i veća svijest o informatičkoj sigurnosti značajni mehanizmi cyber sigurnosti (McCormac, et al., 2016; Hadlington, 2017).

U istraživanju ljudskog i društvenog ponašanja jedna od osobina ličnosti koja se tiče sigurnosti informacija je impulsivnost koja se definiše kao "potreba da se djeluje spontano bez razmišljanja o djelovanju i njegovim posljedicama (Coutlee et al., 2014, Hadlington, 2017). Istraživanja su pokazala da oni pojedinci koji imaju viši nivo impulsivnosti su izloženi većem riziku od onih sa nižim nivoom impulsivnosti (Coutlee et al., 2014; McCoul i Haslam, 2001; Zuckerman i Kuhlman, 2000; Hadlington, 2017). Isto tako, konstatuje Coutlee et al., (2014) da je impulsivnost osobina – komponenta velikog broja kliničkih stanja kao što su ADHD, granični poremećaji ličnosti i poremećaj impulsivne kontrole. Zavisnost od interneta se može uvrstiti u patološke poremećaje (Griffiths, 1998. i 2000; Young, 1998; Hadlington, 2017), ali je potrebno razlikovati zavisnost od interneta od zloupotrebe interneta. Međutim, Stanton (2002) tvrdi "da je zloupotreba interneta na radnom mjestu prirodni nastavak aktivnosti vezanih za ovisnost o internetu". Ali je nesumnjivo da zlupotreba interneta povećava mogućnosti sigurnosti unutar organizacije (Pee et al., 2008; Weatherbee, 2010; Hadlington, 2017) njegovo neetičko korištenje na radnom mjestu doprinosi razvoju cyber kriminala koji uključuje aspekte intelektualnog vlasništva, distribuciju uvredljivog materijala i piraterije na internetu (Chen et al., 2008; Hadlington, 2017).

U tom smislu obrazovanje o informacijskoj sigurnosti mora uključiti efikasne i pouzdane identifikacije u elektronskim komunikacijama polazeći od individualne svijesti subjekata, aspekata njihove ličnosti i sigurnosno – bezbjednosne kulture. Tehnički rizici u cyber sigurnosti se mogu odgovarajućim rješenjima umanjiti, ali ranjivost u ponašanju ostaje permanentno i trajno prisutan problem. Posredovane komunikacije utiču na individualna i grupna ponašanja koja se mogu iskoristiti (zloupotrijebiti) od strane drugih za asocijalna i/ili kriminalna ponašanja. Stoga je posebna uloga i značaj psihologije na razvijanju svijesti o potencijalnim rizicima tzv. ranjivostima i formiranju i projektovanju prihvatljivih modela socijalnog ponašanja koji uključuju dovoljno pouzdane i djelotvorne bihevioralne mjere u zaštiti personalne privatne sigurnosti, ali i sigurnosti organizacije, institucije do online okruženja kome pripadaju.

## Zaključak

Od postanka ljudskog društva brojni su i raznovrsni oblici ugrožavanja sigurnosti – bezbjednosti društva i države, a jedan od osnovnih oblika i načina ugrožavanja je kriminalitet. Kriminalitet se u savremenom društvu, pored klasičnih oblika, manifestuje u novim i savremenim oblicima. Savremeni oblik kriminaliteta je cyber kriminal u virtuelnom prostoru, koji je jedna od njegovih specifičnosti, ali i savremene IT (informacione tehnologije) kao savremeno sredstvo njegovog (iz)vršenja, što otežava proces identifikacije, kako njegovih nosilaca, tako i primarnih i tzv. sekundarnih žrtava ovog oblika kriminala. Nesumnjivo da je ljudski faktor najosjetljivija karika u sistemu sigurnosti – bezbjednosti u cyber (virtuelnom) prostoru.

Psihologija i njene naučne discipline kao što su: forenzička, penološka, inžinjerijska, socijalna psihologija, psihologija kriminaliteta, cyber psihologija, itd., u procesu istraživanja, čovjeka i njegove ljudske prirode, u primjeni stečenih naučnih saznanja u nauci i svim sferama ljudskog i društvenog života imaju bitnu ulogu u prevenciji rizika i ublažavanja posljedica viktimizacije. U tom smislu psihologija ima posebnu ulogu i značaj u izgrađivanju ličnosti i formiranju pozitivnih osobina ličnosti, razvijanju individualne i društvene svijesti o personalnim, grupnim i institucionalnim rizicima od cyber kriminala, potrebi određenih (sa)znanja o elektronskim komunikacionim mrežama i komunikacijama u savremenom društvu, sigurnosno – bezbjednosnoj kulturi i formiranju i razvijanju društveno prihvatljivih modela ponašanja u online komunikacijama kao bitnim faktorima unapređenja cyber sigurnosti u virtuelnom prostoru.

## Literatura


- Allport, G. W. (1985). The historical background of social psychology. In G. Lindzey & E. Aronson (Eds.), The handbook of social psychology (3rd ed., Vol.1, pp.1-46). New York. McGraw-Hill.
- Amoroso, E. (2006). Cyber Security. New Jersey: Silicon Press.
- Aronson, E., Wilson, T. D., Akert R. M. (2005), Socijalna psihologija, Nakladnik, Zagreb: Mate.
- Attrill, A. (2015). Cyberpsychology. Oxford University Press; 1 edition.
- Bryce, J. (2015). Cyberpsychology and Human Factors, Engineering and Technology, Cyberspace Research Unit, School of Psychology, University of Central Lancashire, Preston.
- Buzan, B., Waever, O., & De Wilde, J. (1998). Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.
- Canongia, C., & Mandarino, R. (2014). The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Aplications: 60-80. Hershey, PA:IGI Global.
- Chen, J.V., Chen, C.C., Yang, H.-H., (2008). An empirical avaluation of key factors contributing to internet abuse in the workplace. Ind.Manage. Data Syst. 108 (1), 87-106.
- CNSS. (2010). National Information Assurance Glossary: Committee on National Security Systems (CNSS) Instruction No. 4009
- Coutlee, C.G., Politzer, C.S., Hoyle, R.H., Huettel, S., (2014). An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the Barratt Impulsiveness Scale Version I 1. Arch. Sci. Psychol. 2, 1-12.
- Craigen, D., Diakun - Thibault N., Purse R., (2014). Defining Cybersecurity, Technology Innovation Management Review, 4 (10):13-21.
- Deibert , R., & Rohozinski, R. (2010). Liberation vs. Control: The Future of Cyberspace. Journal of Democracy, 21 (4): 43-57.
- DHS. (2014). A Glossary of Common Cybersecurity Terminology. National Intiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014:
- Griffiths, M. (1998). Internet addiction: does really exist? In Gackenbach, J. (Ed.), Psychology and the Internet: Intrapersonal, Interpersonal and Transpersonal Implications. Academic Press, San Diego, CA, pp.61-75.
- Griffiths, M. (2000). Internet addiction: time to be taken seriously? Addict. Res 8 (5), 413.
- Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon 3, Elsevier Ltd.
- Hadnagy Ch., Eckman, P. (2014). Unmasking the Social Engineer: The Human Element of Security, 1st Edition, Indianapolis Wiley.
- Holt, T.J., Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35 (1), 20-40.

- ITU. (2009). Overview of Sybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU).
- Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A. (2014). Cyber crime Classification and Characteristics. In book: Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter:12, Elsevier Science, pp.149-164.
- John, O.P., Srivastava, S., (1999). Big Five Inventory (BFI). Handbook of Personality: Theory and Research 2, 102-138.
- Kaye, L. K. (2016). Book Review: An Introduction to Cyberpsychology. Cyberpsychology, Behavior, and Social Networking, 19 (4), 294-294.
- Kemmerer, R. A. (2003). Cybersecurity. Proceedings of the 25th IEEE International Conference of Software Engineering: 705-715.
- Leukfeldt, R. (2017). Research Agenda: The human factor in Cybercrime and Cybersecurity. Eleven International Publishing, Netherlands.
- Lewis, J. A. (2006). Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies.
- McGuire, M., Dowling, S. (2013). Chapter 1: Cyber-dependent crimes Cyber crime: A review of the evidence (Home Office Research Report 75 ed., pp. 4-34).
- McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2016). Individual differences and Information Security Awareness. Comput. Human. Behav. 69, 151-156.
- McCoul, M.D., Haslam, M. (2001). Predicting high risk sexual behaviour in heterosexual and homosexual man: the roles of impulsivity and sensation seeking. Pers. Individ. Dif. 31 (8), 1303-1310.
- Oxford University Press. (2014). Oxford Online Dictionary. Oxford: Oxford University Press. October 1.
- Pee, W.G., Woon, I.M.Y., Kankanhalli, A. (2008). Explaining non work related computing in the work place: A comparison of alternative models. Inform. Manage. 45, 120-130.
- Petz, B. (ur.), Furlan, I., Kljajić, S., Kolesarić, V., Krizmanić, M., Szabo, S., Šverko, B., (2005). Psihologijski rječnik, Naklada Slap, Jastrebarsko, Zagreb.
- Public Safety Canada. (2010). Canadas Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada.
- Public Safety Canada. (2014). Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada.
- Saini, H., Rao, Y. Sh., Panda, T.C. (2012). Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications (IJERA),Vol. 2, Issue 2, pp. 202-209.
- Singer, P.W., & Friedman, A. (2013). Cybercecurity and Cyberwar: What Everyone Needs to Know. New York: Oxford University Press.
- Stanton, J. (2002). Company Profile of the Frequent Internet User. Communications of the ACM 45 (1), 55-59.
- Termiz, Dž. (2013), Kritika teorije, Amos Graf, Sarajevo.

- Tikkanen, T. (2017). Human behavior from Cyber Security perspective, Master's Thesis, School of Technology, Master's Degree Programme in Information and Communications Technology, Cyber Security.
- Uebelacker, S., Quiel, S. (2014). The Social Engineering Personality Framework. Workshop on Socio-Technical Aspects in Security and Trust, 24-30.
- Wall, D. (2017). Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century. The ECCLES Centre for American Studies.
- Wederhold, B. (2014), The role of Psychology in Enhancing Cybersecurity, Cyberpsychology, Behavior and Social Networking, Volume 17, Number 2.
- Weatherbee, T.G. (2010). Counterproductive use of technology at work: Information and communications technologies and cyberdeviancy. Hum. Resource Manage. R 20 (1), 35-44.
- Widman, J. (2018). The Emergence of Cyberpsychology. Cyberpsychology: Journal of Psychosocial Research on Cyberspace.Vol.
- Wiener, N. (1948). CYBERNETICS or control and communication in the animal and the machine. second edition, The MIT. Press, Cambridge, Massachusetts.
- Young, K.S. (1998). Internet addiction: The emergence of a new clinical disorder. Cyberpsycholog. Behav. 1 (3), 237-244.
- Zuckerman, M., Kuhlman, D.M. (2000). Personality and risk-taking: common biosocial factors. J. Personal. 68 (6), 999.
- Zvonarević, M. (1978), Socijalna psihologija, Školska knjiga, Zagreb.